UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,211	02/05/2002	Siani Lynne Pearson	B-4487PCT 619499 -6	8087

22879 7590 12/31/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

NOTIFICATION DATE	DELIVERY MODE
12/31/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/049,211	PEARSON ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-22,26,27,29 and 31-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-22,27,29,31,32,34-39,41,42,44,45 and 47* is/are rejected.

7)☒ Claim(s) *26,33,40,43 and 46* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 10/5/2007. Claim 21 is amended. Claims 1-18, 23-25, 28, and 30 are cancelled. Claims 19-22, 26-27, 29, and 31-47 are pending.

Allowable Subject Matter

The indicated allowability of claims 19-22, 26-27, 29, and 31-47 is withdrawn in view of the newly discovered reference(s) to U.S. Patent No. 5,724,425 to Chang et al. and U.S. Patent No. 5,923,884 to Peyret et al. Rejections based on the newly cited reference(s) follow.

Claims 26, 33, 40, 43, and 46 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Objections

Claims 19-22, 26, 27, 29, and 31-47 are objected to because of the following informalities: Please substitute the limitation "operable" to "configured". Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 19-22, 27, 29, 31-32, 35-39, 41-42, 44-45, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levy et al., (U.S. Patent No. 6,092,147 and Levy hereinafter), in view of Chang et al., (U.S. Patent No. 5,724,425 and Chang hereinafter).

Regarding claims 19-21 and 29, Levy discloses a computer platform comprising:

a trusted module which is resistant to internal tampering (col. 7, lines 46-55), means for storing license-related code comprising at least one of a secure executor for checking whether the computer platform or a user thereof is licensed to use particular data and for providing an interface for using the particular data and/or for monitoring its usage, and a secure loader for checking whether the computer platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation, wherein the license-related code includes, for at least one group of particular data, a (or a respective) software executor which specifies the respective group of particular data and which is operable to act as an interface to that group of particular data (col. 7, lines 15-46), the platform includes an operating system that is operable to request the software executor that its respective particular data be used, in

response to such a request, that software executor is operable to request the secure executor to license-check, using its licensing model, whether the computer platform or a user thereof is licensed to use that particular data, in response to such latter request (col. 9, lines 39-67), the secure executor is operable to perform the requested license-check, to sign the result of the license check using a private key of the trusted module, and to respond to that software executor with the signed result, and in response to such a response, that software executor is operable: to check the integrity of the signed result using the public key of the trusted module (col. 6, lines 10-50), and upon a successful integrity check of a successful license-check result, to request the operating system to use that particular data (col. 10, lines 1-25).

Although Levy mentions that the bytecode verification in the bytecode authenticator uses a suitable cryptographic computation such as a digital signature using an asymmetric cryptographic algorithm (col. 6, lines 10-27), it does not explicitly disclose the details of such cryptographic computation.

However, Chang discloses a trusted module (i.e., passport) which stores a third party's public key certificate, means for storing a hashed version of the license-related code signed with the third party's private key (col. 8, lines 25-49), and means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails, and wherein: the software executor (or at least one of the software executors) contains a public key of the trusted module and a licensing model for the respective particular data (col. 8, lines 25-67 and col. 9, lines 1-47)(i.e., during the

verification/integrity checking process, the digital signature in the application writer's license is generated by computing the message of the license and encrypting the message digest using the platform builder's private key. The original message digest can be recovered by decrypting the signature using the platform builder's public key)(col. 9, lines 27-67 and col. 10, lines 1-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Levy with teachings of Chang because it would allow including a valid passport as disclosed by Chang in the tamper-resistant package of Levy. One of ordinary skill in the art would have been motivated by the suggestion of Chang to provide the basis of a trust model and allow computer users to identity and determine the genuineness of a software product based on the information contained in its passport (Chang, col. 6, lines 24-38).

Regarding claims 27, 35-37, 41, 44, and 47, Levy discloses a computer platform comprising:

a trusted module which is resistant to internal tampering (col. 7, lines 46-55), means for storing license-related code comprising at least one of a secure executor for checking whether the computer platform or a user thereof is licensed to use particular data and for providing an interface for using the particular data and/or for monitoring its usage, and a secure loader for checking whether the computer platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation, the secure executor containing at least one licensing model (col. 7, lines 15-

46), means for storing a hashed version of the license-related code signed with the third party's private key, and means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails, wherein the computer platform includes an operating system that is operable to request the software executor that its respective particular data be used, and in response to such a request, the secure executor is operable: to perform a license-check using the, or one of the, licensing models (col. 6, lines 10-50), and upon a successful license-check, to request the operating system to use that particular data (col. 10, lines 1-25).

However, Chang discloses a trusted module (i.e., passport) which stores a third party's public key certificate, means for storing a hashed version of the license-related code signed with the third party's private key (col. 8, lines 25-49), and means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails (col. 8, lines 25-67 and col. 9, lines 19-67). Chang further discloses the computer platform further including a further, [removable], trusted module (col. 3, lines 35-37) containing a user identity (i.e., platform builder's public key), wherein the computer platform is operable to perform an authentication check between the first-mentioned trusted module and the removable trusted module, and wherein, upon license license-checking, the secure executor or software executor is operable to perform the license-check with reference to the user identity (i.e., during the verification/integrity checking process, the digital signature in the application writer's

license is generated by computing the message of the license and encrypting the message digest using the platform builder's private key. The original message digest can be recovered by decrypting the signature using the platform builder's public key) (col. 9, lines 27-67 and col. 10, lines 1-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Levy with teachings of Chang because it would allow including a valid passport as disclosed by Chang in the tamper-resistant package of Levy. One of ordinary skill in the art would have been motivated by the suggestion of Chang to provide the basis of a trust model and allow computer users to identity and determine the genuineness of a software product based on the information contained in its passport (Chang, col. 6, lines 24-38).

Regarding claims 22, 31, 38, 42, and 45, Levy discloses wherein the operating system is programmed to use the particular data only in response to the secure executor or the software executor (col. 10, lines 1-25).

Chang discloses wherein the operating system is programmed to use the particular data only in response to the secure executor or the software executor (col. 8, lines 25-48 and col. 10, lines 6-25).

Regarding claims 31, 32, and 39, Levy discloses wherein the platform includes an operating system programmed to install the particular data only in response to the trusted module (col. 10, lines 1-25).

Chang discloses wherein the platform includes an operating system programmed to install the particular data only in response to the trusted module (i.e., passport)(col. 8, lines 25-48 and col. 10, lines 6-25).

Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Levy et al., (U.S. Patent No. 6,092,147 and Levy hereinafter), in view of Chang et al., (U.S. Patent No. 5,724,425 and Chang hereinafter), in further view of Peyret et al., (U.S. Patent No. 5,923,884 and Peyret hereinafter).

Regarding claim 34, Levy and Chang, alone or in combination, do not disclose wherein, if the check succeeds, the secure loader is operable to perform a virus check on the particular data.

However, Peyret discloses wherein, if the check succeeds, the secure loader is operable to perform a virus check on the particular data (col. 9, lines 33-57).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Levy and Chang with teachings of Peyret because it would allow the secure loader to perform a virus check on the particular data as disclosed by Peyret. One of ordinary skill in the art would have been motivated by the suggestion of Peyret to ensure loading secure applet code (Peyret, col. 9, lines 33-57).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Please see the attached PTO-892 for a complete listing.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

A.S.
Patent Examiner
Group 2131
Dec. 18, 2007